UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/085,346	02/28/2002	Ronald P. Cocchi	PD-2002336	8548

			EXAMINER
20991	7590	03/28/2006	BLUDAU, BRANDON S

THE DIRECTV GROUP INC
PATENT DOCKET ADMINISTRATION RE/R11/A109
P O BOX 956
EL SEGUNDO, CA 90245-0956

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 03/28/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
	10/085,346	COCCHI ET AL.
Office Action Summary	Examiner	Art Unit	
	Brandon S. Bludau	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _03 February 2006_.

2a)☒ This action is **FINAL.**   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-36_ is/are pending in the application.

   4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-36_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

   Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

   Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   a)☐ All b)☐ Some * c)☐ None of:

   1.☐ Certified copies of the priority documents have been received.

   2.☐ Certified copies of the priority documents have been received in Application No. _____.

   3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

   * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

DETAILED ACTION

1.   This office action is in reply to an amendment filed on February 03, 2006. Claims

1,6,10,15,19,24,28, and 33 have been amended. Claims 1-36 are pending.

2.   Examiner has acknowledged and consequently withdraws the 112 rejection

regarding a lack of antecedent basis as the rejected claims have been properly

corrected.

Response to Arguments

3.   Applicant's arguments filed on February 03, 2006 have been fully considered but

they are not persuasive.

Applicant amended the independent claims to include the limitation that "the

identification number is used to limit a cloning attack wherein said cloning attack

comprises copying the identification number to a new CAM". The applicant argues that

the references fail to teach or suggest the use of an identification number wherein the

identification number serves the traditional functions of to determine which key to use,

or to generate the key that is then used, or to address a key delivery message, or to

identify devices that are permitted or excluded from access to services. The Applicant

also argues that the references don't teach that a copying of the so-called identification

number would result in a cloning attack. However, as addressed in the rejections

below, the Examiner explains how Kocher overcomes these arguments.

4.   The Applicant defends the dependent claims as being patentable in support of

their dependence upon the independent claims, however in light of a thorough rejection

of the independent claims the previous rejections hold for the dependent claims.

Claim Rejections - 35 USC § 102

5.   Claims 19,20,22,23,26 are rejected under 35 U.S.C. 102(e) as being anticipated

by Kocher (US Patent 6289455).

6.   As per claim 19, Kocher discloses a conditional access module (CAM), (Fig. 2

#225 wherein the CAM is the cryptographic rights unit) comprising:

a nonvolatile memory component (column 21 lines 13-15), wherein:

the nonvolatile memory component is used to contain state information to provide

desired functionality and enforce one or more security policies for accessing the digital

services (column 10 lines 36-38 and 43-47 wherein the digital services is pay-tv); and

the nonvolatile memory component is protected from modification such that the

nonvolatile memory component is read only (column 10 lines 43-47); and

access to the nonvolatile memory component is isolated (Fig. 2 #265);

a hidden non-modifiable identification number embedded into the nonvolatile

memory component, wherein the identification number uniquely identifies the CAM

(column 7 lines 65-67 column 10 lines 38-40 and 43-45: it can be understood that the

device key necessarily applies to an identification number which as used by the

applicant is a security-related parameter. Moreover, in view of column 10 lines 61-65

and column 11 lines 53-65 it can clearly be seen that the rights key which is generated

from the device key/identification number is used to decrypt/access the content; which

meets the functionality of the identification number as defined by the Applicant.

Moreover in column 12 lines 24-32, 37-40 and 62-66, Kocher explains the use of the

device key to determine permission of access to the services, which also meets a

requirement of the identification number as stated by the Applicant); and

the identification number is used to limit a cloning attack wherein said cloning

attack comprises copying the identification number to a new CAM (column 14 lines 2-9

and column 18 lines 37-45 and column 26 lines 25-40; It can be clearly seen that the

function of the device key which is unique to a device implies a necessary concern that

this key is not copied to another CAM. These passages clearly demonstrate that a

compromised device key would require the cessation of enabling access to those CRUs

containing that particular key. This is necessarily related to the cloning attack as

discussed by the Applicant wherein if an identification number is known to be used by

multiple devices illegally, those devices using that number would no longer be effective);

and

a fixed state custom logic block, wherein the nonvolatile memory component is

not directly accessible via a system bus and access to the nonvolatile memory

component is limited to the custom logic block (Fig. 2 #260 wherein the CryptoFirewall

is the custom logic block).

7.   As per claim 20, Kocher discloses the CAM of claim 19, wherein the nonvolatile

memory component is isolated such that a system input/output module, microprocessor,

or external environment is prevented from direct access to the identification number

(Fig. 2 #265).

8.   As per claim 22, Kocher discloses the CAM of claim 19, wherein the custom logic

block is permitted to read the identification number (Fig.2 #260 wherein the

CryptoFirewall unit is the custom logic block column 21 line 34-35 and the identification

number would be stored in the protected memory #265 as noted in claim 1).

9.   As per claim 23, Kocher discloses the CAM of claim 22, wherein a function

defined in the custom logic block specifies an operation to be performed using the

hidden identification number (column 19 lines 31-35 wherein the BATCH_KEY unique to

the CryptoFirewall column 18 lines 62-64 is used to encrypt secure data in the

protected memory i.e. the identification number alluded to in claim 1).

10.   As per claim 26, Kocher discloses the CAM of claim 19 further comprising a

microprocessor that is configured to embed the identification number into the nonvolatile

memory component (column 21 lines 34-35 wherein the CryptoFirewall is capable of

embedding the identification number as discussed in claim 7).

Claim Rejections - 35 USC § 103

11.   Claims 1,2,4,5,8 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Cohen (US Patent 5282249) in view Kocher (US Patent 6289455).

12.   As per claim 1, Cohen discloses a system for controlling access to digital

services comprising:

        (a) A control center configured to coordinate and provide digital services (see

Fig. 2);

        (b) An uplink center configured to receive the digital services from the control

center and transmit the digital services to a satellite (see Fig. 1/1 #20);

        (c) The satellite configured to:

Receive the digital services from the uplink center (Fig. 1/2 #22);

Process the digital services (Fig. 1/2 #22 wherein processing of digital services is the intrinsic step that allows transmission); and

Transmit the digital services to a subscriber receiver station (Fig. 1/2 #24);

(d) The subscriber receiver station configured to:

Receive the digital services from the satellite (Fig. 1/2 #26);

Control access to the digital services through an integrated receiver/decoder (IRD) (Fig. 1/2 #30);

(e) A conditional access module (CAM) communicatively coupled to the IRD (Fig. 1/2 #32);

but does not disclose wherein the CAM comprises:

a nonvolatile memory component, wherein:

the nonvolatile memory component is used to contain state information to provide desired functionality and enforce one or more security policies for accessing the digital services; and

the nonvolatile memory component is protected from modification such that the nonvolatile memory component is isolated;

a hidden non-modifiable identification number embedded into the nonvolatile memory component, wherein the identification number uniquely identifies the CAM; and

a fixed state custom logic block, wherein the nonvolatile memory component is not directly accessible via a system bus and access to the nonvolatile memory component is limited to the custom logic block.

Kocher discloses wherein the CAM (Fig. 2 #225 wherein the CAM is the cryptographic rights unit) comprises:

a nonvolatile memory component (column 21 lines 13-15), wherein:

the nonvolatile memory component is used to contain state information to provide desired functionality and enforce one or more security policies for accessing the digital services (column 10 lines 36-38 and 43-47 wherein the digital services is pay-tv); and

the nonvolatile memory component is protected from modification such that the nonvolatile memory component is read only (column 10 lines 43-47); and

access to the nonvolatile memory component is isolated (Fig. 2 #265);

a hidden non-modifiable identification number embedded into the nonvolatile memory component, wherein the identification number uniquely identifies the CAM (column 7 lines 65-67 column 10 lines 38-40 and 43-45: it can be understood that the device key necessarily applies to an identification number which as used by the applicant is a security-related parameter. Moreover, in view of column 10 lines 61-65 and column 11 lines 53-65 it can clearly be seen that the rights key which is generated from the device key/identification number is used to decrypt/access the content; which meets the functionality of the identification number as defined by the Applicant. Moreover in column 12 lines 24-32, 37-40 and 62-66, Kocher explains the use of the device key to determine permission of access to the services, which also meets a requirement of the identification number as stated by the Applicant); and

the identification number is used to limit a cloning attack wherein said cloning attack comprises copying the identification number to a new CAM (column 14 lines 2-9

and column 18 lines 37-45 and column 26 lines 25-40; It can be clearly seen that the function of the device key which is unique to a device implies a necessary concern that this key is not copied to another CAM. These passages clearly demonstrate that a compromised device key would require the cessation of enabling access to those CRUs containing that particular key. This is necessarily related to the cloning attack as discussed by the Applicant wherein if an identification number is known to be used by multiple devices illegally, those devices using that number would no longer be effective); and

a fixed state custom logic block, wherein the nonvolatile memory component is not directly accessible via a system bus and access to the nonvolatile memory component is limited to the custom logic block (Fig. 2 #260 wherein the CryptoFirewall is the custom logic block).

Kocher is analogous art because it discusses a method and apparatus for preventing piracy of digital content including the use of a smart card.

It would have been obvious at the time of the invention to include the features of the CAM found in Kocher in the smart card used by Cohen to control access to the broadcasted data.

Motivation for one to modify Cohen as discussed above would have been to improve the security of systems used to distribute and protect digital content (from piracy or attackers) as taught in Kocher (column 5 lines 55-56).

13.   As per claim 2, Kocher discloses the system of claim 1, wherein the nonvolatile memory component is isolated such that a system input/output module, microprocessor,

or external environment is prevented from direct access to the identification number

(Fig. 2 #265).

14.   As per claim 4, Kocher discloses the system of claim 1, wherein the custom logic

block is permitted to read the identification number (Fig.2 #260 wherein the

CryptoFirewall unit is the custom logic block column 21 line 34-35 and the identification

number would be stored in the protected memory #265 as noted in claim 1).

15.   As per claim 5, Kocher discloses the system of claim 4, wherein a function

defined in the custom logic block specifies an operation to be performed using the

hidden identification number (column 19 lines 31-35 wherein the BATCH_KEY is unique

to the CryptoFirewall column 18 lines 62-64 and is used to encrypt secure data in the

protected memory i.e. the identification number alluded to in claim 1).

16.   As per claim 8, Kocher discloses the system of claim 1 further comprising a

microprocessor that is configured to embed the identification number into the nonvolatile

memory component (column 21 lines 34-35 wherein the CryptoFirewall is capable of

embedding the identification number as discussed in claim 7).

17.   Claims 3,6,7 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Cohen (US Patent 5282249) in view of Kocher (US Patent 6289455) and further in view

of Pitts (US PgPub 20020145931).

18.   As per claim 3, Cohen/Kocher disclose the system of claim 1, but do not disclose

wherein the identification number is embedded after manufacturing.

    Pitts does disclose wherein the identification number is embedded after

manufacturing (paragraph [0011] lines 1-4 wherein Pitts specifically notes the ability to

load data into the secure memory clearly after manufacturing of the device wherein the

identification number is alluded to in paragraph [0003] wherein an identification number

would clearly enable special access and authorize transactions).

Pitts is analogous art because it discloses a method of securing data in an

integrated circuit.

It would have been obvious for one of ordinary skill in the art to modify

Cohen/Kocher to include the mechanism so that the identification number could be

embedded after manufacturing.

Motivation for one to modify Cohen/Kocher as described above would have been

to provide a means for preventing "external access to secure data stored in the memory

array" as taught in Pitts (paragraph [0013] lines 11-14).

19.   As per claim 6, Cohen/Kocher discloses the system of claim 1 but does not

disclose it further comprising a onetime programmable memory protected by a

hardware fuse that isolates the identification number from the microprocessor after the

identification number is written.

Pitts does disclose a onetime programmable memory protected by a hardware

fuse that isolates the identification number from the microprocessor after the

identification number is written (paragraph [0013] lines 4-7 and 11-14).

Pitts is analogous art because it discloses a method of securing data in an

integrated circuit.

It would have been obvious to one of ordinary skill in the art to modify

Cohen/Kocher to include securing the data by blowing an input fuse as taught in Pitts.

Motivation for one to modify Cohen/Kocher as discussed above would have been to provide the means for one to secure private data that may be used to enable special access to specific functions, as taught in Pitts (paragraph [0003]).

20.   As per claim 7, Cohen/Kocher disclose the system of claim 1 (wherein the CryptoFirewall controls access to the protected memory), but do not disclose wherein the custom logic block (CryptoFirewall) is configured to embed the identification number into the nonvolatile memory component.

Pitts does disclose logic that is capable of embedding the identification number into the secure memory array (paragraph [0010] lines 8-11 wherein the secure memory periphery has similar functionality to the CryptoFirewall).

Pitts is analogous art because it discloses a method of securing data in an integrated circuit.

It would have been obvious for one of ordinary skill in the art to modify Kocher to include the mechanism so that the identification number could be embedded by the custom logic block.

Motivation for one to modify Kocher as described above would have been to provide a means for preventing "external access to secure data stored in the memory array" as taught in Pitts (paragraph [0013] lines 11-14).

21.   Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Cohen (US Patent 5282249) in view Kocher (US Patent 6289455) and further in view of Barth (US Patent 6334216).

22.   As per claim 9, Cohen/Kocher disclose the system of claim 1 with a hidden non-modifiable identification number, but do not disclose wherein access to the digital services is rejected when the hidden non-modifiable identification number is on a list of unauthorized identification numbers.

Barth does disclose wherein access to digital services is rejected when an identification number is on a list of unauthorized identification numbers (column 4 lines 33-45).

Barth is analogous art because it discloses a method of gaining access to services based on an identification number utilized in an access card.

It would have been obvious for one of ordinary skill in the art at the time of the invention to modify Cohen/Kocher to include the method of comparing an identification number to a list of unauthorized numbers before granting access.

Motivation for one to modify Cohen/Kocher as discussed above would have been to allow system management to prevent access to the services if the corresponding number is reported as lost or if the user is delinquent in his obligations for the services offered as taught in Barth (column 3 lines 37-42).

23.   Claims 10,11,13,14,17,18, 27,28,29,31,32,35,36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher (US Patent 6289455) in view of Barth (US Patent 6334216).

24.   As per claim 10, Kocher discloses a method for limiting unauthorized access to digital services comprising:

Embedding a hidden non-modifiable identification number into a nonvolatile

memory component (column 21 lines 13-15 and column 18 lines 37-45 wherein the

identification number is the serial number alluded to and which is stored in the protected

memory and is non-modifiable in the same manner as the unique BATCH_KEY

described in column 18 lines 49-52; see also claim 1), wherein:

The nonvolatile memory component is used to contain state information to

provide desired functionality and enforce one or more security policies for accessing the

digital services (column 10 lines 36-38 and 43-47 wherein the digital services is pay-tv);

The hidden non-modifiable identification number uniquely identifies a device

containing the nonvolatile memory component (column 18 lines 37-45 see also claim 1);

and

the identification number is used to limit a cloning attack wherein said cloning

attack comprises copying the identification number to a new CAM (column 14 lines 2-9

and column 18 lines 37-45 and column 26 lines 25-40; It can be clearly seen that the

function of the device key which is unique to a device implies a necessary concern that

this key is not copied to another CAM. These passages clearly demonstrate that a

compromised device key would require the cessation of enabling access to those CRUs

containing that particular key. This is necessarily related to the cloning attack as

discussed by the Applicant wherein if an identification number is known to be used by

multiple devices illegally, those devices using that number would no longer be effective);

and

Isolating access to the nonvolatile memory component such that access to the

nonvolatile memory component is limited to a fixed state custom logic block (Fig. 2 #260

wherein the CryptoFirewall is the custom logic block as described in column 21 lines 34-

35), the nonvolatile memory component is protected such that the nonvolatile memory

component is read only (column 10 lines 43-47), and the nonvolatile memory

component is not directly accessible via a system bus (Fig. 2 #260).

But does not disclose wherein access to the digital services is based on access

rights associated with the hidden non-modifiable identification number.

Barth does disclose wherein access to the digital services is based on access

rights associated with an identification number (column 4 lines 33-45 wherein the

access rights is whether it is associated with a blocking note).

Barth is analogous art because it discloses a method of gaining access to

services based on an identification number utilized in an access card.

It would have been obvious for one of ordinary skill in the art at the time of the

invention to modify Kocher to include the method of comparing an identification number

to a list of unauthorized numbers and their access rights before granting access.

Motivation for one to modify Kocher as discussed above would have been to

allow system management to prevent access to the services if the corresponding

number is reported as lost or if the user is delinquent in his obligations for the services

offered as taught in Barth (column 3 lines 37-42).

25.   As per claim 11, Kocher discloses the method of claim 10, wherein the

nonvolatile memory component is isolated by preventing a system input/output module,

microprocessor, or external environment from direct access to the identification number

(Fig. 2 #265).

26.   As per claim 13, Kocher discloses the method of claim 10, wherein the custom

logic block is permitted to read the identification number (Fig.2 #260 wherein the

CryptoFirewall unit is the custom logic block column 21 line 34-35 and the identification

number would be stored in the protected memory #265 as noted in claim 1).

27.   As per claim 14, Kocher discloses the method of claim 13, wherein a function

defined in the custom logic block specifies an operation to be performed using the

hidden identification number (column 19 lines 31-35 wherein the BATCH_KEY is unique

to the CryptoFirewall column 18 lines 62-64 and is used to encrypt secure data in the

protected memory i.e. the identification number alluded to in claim 1).

28.   As per claim 17, Kocher discloses the method of claim 10 wherein a

microprocessor embeds the identification number into the nonvolatile memory

component (column 21 lines 34-35 wherein the CryptoFirewall is capable of embedding

the identification number as discussed in claim 7).

29.   As per claim 18, Kocher discloses the method of claim 10, further comprising

rejecting access to the digital services when the hidden non-modifiable identification

number is on a list of unauthorized identification numbers (column 4 lines 33-45).

30.   Claim 27 is rejected because it discusses the same subject matter as claim 9.

31.   Claim 28 is rejected because it discusses the same subject matter as claim 10.

32.   Claim 29 is rejected because it discusses the same subject matter as claim 11.

33.   Claim 31 is rejected because it discusses the same subject matter as claim 13.

34.   Claim 32 is rejected because it discusses the same subject matter as claim 14.

35.   Claim 35 is rejected because it discusses the same subject matter as claim 17.

36.   Claim 36 is rejected because it discusses the same subject matter as claim 18.

37.   Claims 12,15,16,30,33,34 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Kocher (US Patent 6289455) in view of Barth (US Patent6334216)

and further in view of Pitts (US PgPub 20020145931).

38.   As per claim 12, Kocher/Barth disclose the method of claim 10, but do not

disclose wherein the identification number is embedded after manufacturing.

Pitts does disclose wherein the identification number is embedded after

manufacturing (paragraph [0011] lines 1-4 wherein Pitts specifically notes the ability to

load data into the secure memory clearly after manufacturing of the device wherein the

identification number is alluded to in paragraph [0003] wherein an identification number

would clearly enable special access and authorize transactions).

Pitts is analogous art because it discloses a method of securing data in an

integrated circuit.

It would have been obvious for one of ordinary skill in the art to modify Kocher to

include the mechanism so that the identification number could be embedded after

manufacturing.

Motivation for one to modify Kocher/Barth as described above would have been

to provide a means for preventing "external access to secure data stored in the memory

array" as taught in Pitts (paragraph [0013] lines 11-14).

39.   As per claim 15, Kocher/Barth disclose the method of claim 10, but do not

disclose wherein the identification number is embedded using a onetime programmable

memory protected by a hardware fuse that isolates the identification number from a

microprocessor after the identification number is written.

Pitts does disclose a onetime programmable memory protected by a hardware

fuse that isolates the identification number from the microprocessor after the

identification number is written (paragraph [0013] lines 4-7 and 11-14).

Pitts is analogous art because it discloses a method of securing data in an

integrated circuit.

It would have been obvious to one of ordinary skill in the art to modify

Kocher/Barth to include securing the data by blowing an input fuse as taught in Pitts.

Motivation for one to modify Kocher as discussed above would have been to

provide the means for one to secure private data that may be used to enable special

access to specific functions, as taught in Pitts (paragraph [0003]).

40.   As per claim 16, Kocher/Barth disclose the method of claim 10 (wherein the

CryptoFirewall controls access to the protected memory), but do not disclose wherein

the custom logic block (CryptoFirewall) embeds the identification number into the

nonvolatile memory component.

Pitts does disclose logic that embeds the identification number into the secure

memory array (paragraph [0010] lines 8-11 wherein the secure memory periphery has

similar functionality to the CryptoFirewall).

Pitts is analogous art because it discloses a method of securing data in an integrated circuit.

It would have been obvious for one of ordinary skill in the art to modify Kocher/Barth to include the mechanism so that the identification number could be embedded by the custom logic block.

Motivation for one to modify Kocher/Barth as described above would have been to provide a means for preventing "external access to secure data stored in the memory array" as taught in Pitts (paragraph [0013] lines 11-14).

41.   Claim 30 is rejected because it discusses the same subject matter as claim 12.

42.   Claim 33 is rejected because it discusses the same subject matter as claim 15.

43.   Claim 34 is rejected because it discusses the same subject matter as claim 16.

44.   Claims 21,24,25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher (US Patent 6289455) in view of Pitts (US PgPub 20020145931).

45.   Claim 21 is rejected because it discusses the same subject matter as claim 3.

46.   Claim 24 is rejected because it discusses the same subject matter as claim 6.

47.   Claim 25 is rejected because it discusses the same subject matter as claim 7.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later

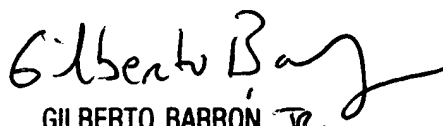than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Brandon S. Bludau whose telephone number is 571-

272-3722. The examiner can normally be reached on Monday -Friday 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number

for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

Brandon S Bludau
Examiner
Art Unit 2132

BB
***

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100